REMARKS / DISCUSSION OF ISSUES

Claims 1-20 are pending in the application.

The Office action objects to the specification; the specification is correspondingly amended herein. No new matter is added, because the application as originally filed includes "a computer program product".

The Office action repeats the rejection of:

claims 1, 9-12, and 16-19 under 35 U.S.C. 103(a) over Leighton et al. (USP 5,519,778, hereinafter Leighton) and Hoffstein et al. (USP 6,076,163, hereinafter Hoffstein);

claims 2-4 and 20 under 35 U.S.C. 103(a) over Leighton, Hoffstein, and Matyas et al. (USP 5,953,420); and

claims 13-15 under 35 U.S.C. 103(a) over Leighton, Hoffstein, and Menezes et al. (Handbook of Applied Cryptography). The applicants respectfully traverse these rejections for the reasons stated in the applicants' response of 20 March 2008.

Each of these rejections relies on Leighton and Hoffstein for teaching the elements of the applicants' independent claims 1, 16, 17, and 19. However, neither Leighton nor Hoffstein teaches or suggests calculating a common secret between two parties as a product of two symmetrical polynomials, as specifically claimed in each of the applicants' independent claims.

The Office action acknowledges that Leighton fails to provide this teaching, and asserts that Hoffstein teaches calculating a secret as a product of two symmetrical polynomials at column 3, lines 31-46 and FIG. 3. The applicants respectfully disagree with this assertion.

In response to the applicants' prior remarks, the Office action asserts that the polynomials g(x) and (f(x) + c(x)) of Hoffstein are symmetrical polynomials (Office action, page 3, lines 10-11); this is not correct. As is well known in the art:

> "In mathematics, a symmetric polynomial is a polynomial $P(X_1, X_2, \ldots, X_n)$ in n variables, such that if any of the variables are interchanged, one obtains the same polynomial. Formally, P is a *symmetric polynomial*, if for any permutation σ of the subscripts 1, 2, ..., n one has $P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}) = P(X_1, X_2, \ldots, X_n)$." (http://en.wikipedia.org.)

By definition, a polynomial in one variable, such as Hoffstein's g(x) and (f(x) + c(x)), cannot be a symmetric polynomial, because a symmetric polynomial is defined with regard to an interchange of variables, and a single variable cannot be 'interchanged'.

The Examiner's attention is requested to page 2, lines 17-25, wherein the applicants show that the polynomial P in two variables, x and y, exhibits the property that P(x,y) = P(y,x), which conforms to the above definition of a symmetric polynomial: an interchange of variables x and y produces the same polynomial.

Because a basic mathematical premise of the Office action's rejections of claims 1-4, and 9-20 under 35 U.S.C. 103(a) is incorrect, the applicants respectfully maintain that the Office action has not established a prima facie case, and therefore each of the rejections in this Office action should be withdrawn.

In view of the foregoing, the applicants respectfully request that the Examiner withdraw the objection(s) and/or rejection(s) of record, allow all the pending claims, and find the application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

/Robert M. McDermott/
Robert M. McDermott, Esq.
Reg. 41,508
804-493-0707

Please direct all correspondence to:
Corporate Counsel
U.S. PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001